

### **Amendments to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application.

### **Listing of Claims:**

1. (Currently Amended) A method of obstructing identity crimes, the method comprising:
  - obtaining at a verification system a list of at least two identity verifiers, each identity verifier to be used for no more than one transaction;
  - linking at the verification system the list of identity verifiers to at least one numerical identifier associated with a registered user, the registered user selected from the group consisting of persons and entities;
  - providing the list of identity verifiers from the verification system to the registered user;
  - enabling the registered user to provide security ~~information~~ messages to the verification system to be associated with ~~one of the~~ identity verifiers, ~~the information~~ each security message pertaining to an intended transaction;
  - receiving at the verification system a numerical identifier from a requesting party, the requesting party having obtained the numerical identifier from a transaction initiator claiming to be associated with the numerical identifier;
  - receiving at the verification system an identity verifier from the requesting party, the requesting party having obtained the identity verifier from the transaction initiator claiming to be associated with the numerical identifier;
  - determining at the verification system whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier;
  - communicating information from the verification system to the requesting party indicating whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier; and
  - sending from the verification system to the requesting party any security message associated with the received identity verifier to enable the requesting party to compare the security message with a transaction being conducted by the transaction initiator.

2. (Previously Presented) The method of claim 1 wherein the communicating information step signals that the received identity verifier has not been used before and is within the list of identity verifiers linked to the received numerical identifier by sending a verification transaction identifier to the requesting party.

3. (Previously Presented) The method of claim 1 further comprising:

(a) determining whether the identity verifier received from the requesting party has been used before; and

(b) communicating information to the requesting party signaling whether the identity verifier has been used before.

4. (Previously Presented) The method of claim 2 further comprising archiving the identity verifier and the verification transaction identifier.

5. (Currently Amended) The method of claim 1 further comprising:

(a) storing public information about the registered user ~~whose identity is to be verified~~;

(b) creating at least two categories of requesting parties;

(c) receiving instructions from the registered user regarding what public information is allowed to be released to each of the at least two categories of requesting party;

(d) determining the category of the requesting party;

(e) communicating the appropriate public information to the requesting party pursuant to the instructions from the registered user.

6. (Original) The method of claim 1 wherein the at least one numerical identifier is a social security number.

7. (Original) The method of claim 1 wherein the at least one numerical identifier is a drivers license number.

8. (Original) The method of claim 1 wherein the at least one numerical identifier is a bank account number.
9. (Original) The method of claim 1 wherein the at least one numerical identifier is a phone number.
10. (Original) The method of claim 1 wherein the at least one numerical identifier is a credit card number.
11. (Previously Presented) The method of claim 1 further comprising receiving a uniqueness suffix and wherein determining whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier further comprises determining whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier and the received uniqueness suffix.
12. (Previously Presented) The method of claim 1 wherein receiving a numerical identifier, receiving an identity verifier and communicating information to the requesting party are performed by voice communications over a phone line.
13. (Previously Presented) The method of claim 1 wherein receiving a numerical identifier, receiving an identity verifier and communicating information to the requesting party are performed through electronic communication through a wide area network.
14. (Previously Presented) A method of determining whether an identity verifier is required to be submitted in a particular transaction, the method comprising:
  - (a) obtaining a list of at least two identity verifiers, each identity verifier to be used for no more than one transaction;
  - (b) linking the list of identity verifiers to at least one unique numerical identifier wherein the numerical identifier is associated with a registered user selected from a group consisting of persons and entities;
  - (c) creating categories of transactions;

(d) receiving instructions from the registered user designating the categories of transactions that require an identity verifier and designating the categories of transactions that do not require an identity verifier;

(e) receiving a numerical identifier from a requesting party, the requesting party having obtained the numerical identifier from a transaction initiator claiming to be associated with the numerical identifier;

(f) receiving information from the requesting party specifying the type of transaction occurring;

(g) determining whether the transaction requires the use of an identity verifier; and

(h) communicating information to the requesting party wherein the information communicated indicates whether an identity verifier is required for the specified transaction.

15-26. (Cancelled)

27. (Currently Amended) A method of obstructing identity crimes, the method comprising: associating a plurality of identity verifiers with a registered user, each of the identity verifiers to be used for a single transaction;

receiving from the registered user at least one security message, each security message corresponding to one of the plurality of identity verifiers;

associating each security message provided by the registered user to the corresponding identity verifier;

receiving one of the plurality of identity verifiers from a requesting party, the requesting party having received the one identity verifier from a transaction initiator;

determining whether the one identity verifier received from the requesting party is associated with a corresponding security message; and

transmitting to the requesting party ~~an indication of whether the one~~ any corresponding security message associated with the one identity verifier received from the requesting party to allow the requesting party to view the corresponding security message provided by the registered user is associated with a corresponding security message.

28. (Currently Amended) The method of claim 27, wherein transmitting the security message associated with the received identity verifier includes enabling the requesting party to

compare the message pertaining to the transaction with a transaction initiated by the transaction initiator.

29. (Currently Amended) A method of protecting numerical identifiers associated with registered users, the method comprising:

- obtaining at least one registered user;
- obtaining a list for each registered user, each list including at least one numerical identifier, each numerical identifier included in the list associated with the registered user;
- obtaining at least two identity verifiers for each registered user, each identity verifier to be used in only one transaction;
- associating each of the at least two identity verifiers with the corresponding registered user; and
- transmitting to each registered user the at least two identity verifiers associated with the registered user, each of the identity verifiers enabling the registered user to verify to a requesting party via a verification system any ~~the~~ numerical identifier from the list, and each of the identity verifiers capable of verifying the selected numerical identifier.

30. (Previously Presented) The method of claim 29, wherein at least one numerical identifier in at least one of the lists includes a unique suffix enabling the numerical identifier to be associated uniquely with the registered user, wherein removing the unique suffix from the numerical identifier would yield a shared numerical identifier.

31. (Previously Presented) The method of claim 29, wherein the numerical identifier is selected from the group consisting of social security numbers, bank account numbers, credit card numbers, drivers license numbers, phone numbers, and Internet addresses.

32. (Previously Presented) The method of claim 29, further comprising:

- determining a numerical identifier type for each numerical identifier on the list; and
- associating each numerical identifier on the list with the respective numerical identifier type.

33. (Previously Presented) A system for protecting numerical identifiers of registered users, the system comprising:

an input device configured to obtain a corresponding list for each of a plurality of registered users, each list including at least one numerical identifier, the input device being further configured to obtain at least two identity verifiers for each of the plurality of registered users;

a database configured to associate each of the plurality of registered users with the corresponding list of the at least one numerical identifier, the database being further configured to associate each of the at least two identity verifiers with the corresponding registered user; and

a communications device configured to transmit to each registered user the at least two identity verifiers associated with the registered user, each of the identity verifiers enabling the registered user to verify to requesting parties any numerical identifier selected from the list by the registered user, and each of the identity verifiers being capable of verifying the selected numerical identifier in any one transaction.

34. (Currently Amended) A verification system of obstructing configured to obstruct identity crimes, the verification system comprising:

an input device configured to obtain a list of at least two identity verifiers to be associated with a registered user, the registered user selected from the group consisting of persons and entities, each identity verifier to be used for no more than one transaction, the input device further configured to enable the registered user to provide a security message to be associated with one of the identity verifiers, the security message indicating information pertaining to an intended transaction;

a database configured to link the list of identity verifiers to at least one numerical identifier associated with the registered user, the database further configured to link a security message to one of the identity verifiers if the registered user has provided such a security message;

a communication device configured to receive a numerical identifier and an identity verifier from a requesting party, the requesting party having obtained the numerical identifier and the identity verifier from a transaction initiator claiming to be associated with the numerical identifier, the communication device further configured to transmit to the requesting party

information indicating whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier and whether a security message has been associated with the received identity verifier; and

a processing device configured to determine whether the received identity verifier is within the list of identity verifiers linked in the database to the received numerical identifier, the processing device further configured to determine whether the received identity verifier is associated with a security message.